(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-20720
(P2009-20720A)
(43)公開日　平成21年1月29日(2009.1.29)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/24	(2006.01)	G06F 12/14	560B	5B017

審査請求 有　請求項の数 11　ＯＬ　（全 22 頁）

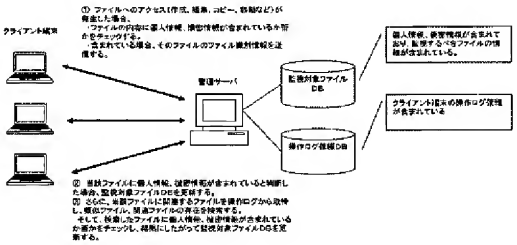
(21)出願番号　特願2007-183123 (P2007-183123)
(22)出願日　平成19年7月12日 (2007.7.12)

(71)出願人　599108242
Ｓｋｙ株式会社
大阪府大阪市淀川区宮原三丁目４番３０号
ニツセイ新大阪ビル
(74)代理人　100088214
弁理士　生田　哲郎
(74)代理人　100134588
弁理士　吉浦　洋一
(72)発明者　和仁　稔
大阪府大阪市淀川区宮原三丁目４番３０号
ニッセイ新大阪ビル　Ｓｋｙ株式会社内
(72)発明者　本永　直樹
大阪府大阪市淀川区宮原三丁目４番３０号
ニッセイ新大阪ビル　Ｓｋｙ株式会社内

Ｆターム(参考)　5B017 AA08　BB06　CA16

(54)【発明の名称】ファイル管理システム

(57)【要約】　（修正有）
【課題】組織において使用されているコンピュータシステムで、監視対象となる個人情報や機密情報などを含むファイルの所在場所を管理するファイル管理システムを提供する。
【解決手段】監視対象ファイル記憶部と、コンピュータシステムを構成するコンピュータ端末の操作ログ情報を用いて、該操作ログ情報におけるファイルに対してアクセスがあったかを、該操作ログ情報の操作内容により判定するアクセス判定部と、アクセスがあったと判定したファイルを記憶するコンピュータ端末に対して、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部と、ファイルが個人情報または機密情報を含むファイルであるとの検索結果をコンピュータ端末から受け取ると、ファイルの所在場所を監視対象ファイル記憶部に記憶させる監視対象ファイル登録処理部と、を有するファイル管理システムである。
【選択図】図１



【特許請求の範囲】
【請求項1】
コンピュータシステムで利用されている個人情報または機密情報を含むファイルの所在場所を管理するファイル管理システムであって、
前記ファイル管理システムは、
監視対象となる個人情報または機密情報を含むファイルの所在場所を記憶する監視対象ファイル記憶部と、
前記コンピュータシステムを構成するコンピュータ端末の操作ログ情報を用いて、該操作ログ情報におけるファイルに対してアクセスがあったかを、該操作ログ情報の操作内容により判定するアクセス判定部と、
前記アクセスがあったと判定したファイルを記憶するコンピュータ端末に対して、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部と、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果を前記コンピュータ端末から受け取ると、前記ファイルの所在場所を前記監視対象ファイル記憶部に記憶させる監視対象ファイル登録処理部と、
を有することを特徴とするファイル管理システム。
【請求項2】
前記ファイル管理システムは、更に、
各コンピュータ端末の操作ログ情報を記憶する操作ログ情報記憶部と、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果を前記コンピュータ端末から受け取ると、前記ファイルの類似ファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報に基づいて検索する類似ファイル検索部と、
を有することを特徴とする請求項１に記載のファイル管理システム。
【請求項3】
前記ファイル管理システムは、更に、
各コンピュータ端末の操作ログ情報を記憶する操作ログ情報記憶部と、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果を前記コンピュータ端末から受け取ると、前記ファイルの関連ファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報に基づいて検索する関連ファイル検索部と、
を有することを特徴とする請求項１または請求項２に記載のファイル管理システム。
【請求項4】
コンピュータシステムで利用されている個人情報または機密情報を含むファイルの所在場所を管理するファイル管理システムであって、
前記ファイル管理システムは、
監視対象となる個人情報または機密情報を含むファイルのファイル識別情報と所在場所を記憶する監視対象ファイル記憶部と、
前記コンピュータシステムを構成する各クライアント端末から操作ログ情報を受け付ける操作ログ情報受付部と、
前記操作ログ情報を用いて、該操作ログ情報における操作内容が、予め定められたアクセス処理であったかを判定し、前記予め定められたアクセス処理であったと判定した場合には、該操作ログ情報におけるファイル識別情報とファイルの所在場所とを抽出するアクセス判定部と、
前記抽出したファイルの所在場所に該当するコンピュータ端末に対して前記抽出したファイル識別情報を渡すことで、前記ファイル識別情報に対応するファイルが、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部と、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、前記ファイル識別情報と、前記ファイル識別情報に対応する所在場所とを前記監視対象ファイル記憶部に記憶させる監視対象ファイル登録処理部と、

を有することを特徴とするファイル管理システム。
【請求項5】
　前記ファイル管理システムは、更に、
前記操作ログ情報受付部で受け付けた操作ログ情報を記憶する操作ログ情報記憶部と、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、そのファイル識別情報に基づいて、同一または類似のファイル識別情報を有するほかのファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報から検索し、前記検索した類似ファイルのファイル識別情報とその所在場所とを該操作ログ情報から抽出する類似ファイル検索部、を有しており、
前記検索要求部は、
前記類似ファイル検索部が抽出した類似ファイルの所在場所に該当するコンピュータ端末に対して前記抽出した類似ファイルのファイル識別情報を渡すことで、前記類似ファイルが、個人情報または機密情報を含むかの検索を要求する、
ことを特徴とする請求項４に記載のファイル管理システム。
【請求項6】
　前記ファイル管理システムは、更に、
前記操作ログ情報受付部で受け付けた操作ログ情報を記憶する操作ログ情報記憶部と、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、そのファイル識別情報に対応するファイルに関連するほかのファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報から検索し、前記検索した関連ファイルのファイル識別情報とその所在場所とを該操作ログ情報から抽出する関連ファイル検索部、を有しており、
前記検索要求部は、
前記関連ファイル検索部が抽出した関連ファイルの所在場所に該当するコンピュータ端末に対して前記抽出した関連ファイルのファイル識別情報を渡すことで、前記関連ファイルが、個人情報または機密情報を含むかの検索を要求する、
ことを特徴とする請求項４または請求項５に記載のファイル管理システム。
【請求項7】
　前記ファイル管理システムは、更に、
前記コンピュータシステムにおいて使用されているファイルのファイル識別情報とその所在場所とを記憶するファイルインデックス記憶部と、
前記操作ログ情報受付部で受け付けた操作ログ情報の操作内容に基づいて、ファイルに対して、追加、変更、削除のいずれかがされたかを判定し、判定した場合には、該ファイルの操作ログ情報におけるファイル識別情報または所在場所に基づいて、前記ファイルインデックス記憶部のファイル識別情報及び／又は所在場所を更新するファイルインデックス処理部と、
前記操作ログ情報受付部で受け付けた操作ログ情報を記憶する操作ログ情報記憶部と、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、そのファイル識別情報に基づいて、同一または類似のファイル識別情報を有するほかのファイルが存在するかを、前記ファイルインデックス記憶部に記憶するファイル識別情報から検索し、前記検索した類似ファイルの所在場所を前記ファイルインデックス記憶部から抽出する類似ファイル検索部と、を有しており、
前記検索要求部は、
前記類似ファイル検索部が抽出した類似ファイルの所在場所に該当するコンピュータ端末に対して前記抽出した類似ファイルのファイル識別情報を渡すことで、前記類似ファイルが、個人情報または機密情報を含むかの検索を要求する、
ことを特徴とする請求項４に記載のファイル管理システム。
【請求項8】

前記ファイル管理システムは、更に、
前記コンピュータシステムにおいて使用されているファイルのファイル識別情報とその所在場所とを記憶するファイルインデックス記憶部と、
前記操作ログ情報受付部で受け付けた操作ログ情報の操作内容に基づいて、ファイルに対して、追加、変更、削除のいずれかがされたかを判定し、判定した場合には、該ファイルの操作ログ情報におけるファイル識別情報または所在場所に基づいて、前記ファイルインデックス記憶部のファイル識別情報及び／又は所在場所を更新するファイルインデックス処理部と、
前記操作ログ情報受付部で受け付けた操作ログ情報を記憶する操作ログ情報記憶部と、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、そのファイル識別情報に対応するファイルに関連するほかのファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報から検索し、前記検索した関連ファイルのファイル識別情報を該操作ログ情報から抽出し、抽出した関連ファイルのファイル識別情報に対応する所在場所を前記ファイルインデックス記憶部から抽出する関連ファイル検索部と、を有しており、
前記検索要求部は、
前記関連ファイル検索部が抽出した関連ファイルの所在場所に該当するコンピュータ端末に対して前記抽出した関連ファイルのファイル識別情報を渡すことで、前記関連ファイルが、個人情報または機密情報を含むかの検索を要求する、
ことを特徴とする請求項４または請求項７に記載のファイル管理システム。
【請求項9】
前記ファイル管理システムは、更に、
前記監視対象ファイル記憶部に記憶したファイル所在場所のファイルに対する操作ログ情報を監視する監視処理部、
を有することを特徴とする請求項１から請求項８のいずれかに記載のファイル管理システム。
【請求項10】
監視対象となる個人情報または機密情報を含むファイルの所在場所を記憶する記憶装置を有するコンピュータ端末を、
コンピュータシステムを構成するコンピュータ端末の操作ログ情報を用いて、該操作ログ情報におけるファイルに対してアクセスがあったかを、該操作ログ情報の操作内容により判定するアクセス判定部、
前記アクセスがあったと判定したファイルを記憶するコンピュータ端末に対して、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果を前記コンピュータ端末から受け取ると、前記ファイルの所在場所を前記記憶装置に記憶させる監視対象ファイル登録処理部、
として機能させることを特徴とするファイル管理プログラム。
【請求項11】
監視対象となる個人情報または機密情報を含むファイルのファイル識別情報と所在場所を記憶する記憶装置を有するコンピュータ端末を、
コンピュータシステムを構成する各クライアント端末から操作ログ情報を受け付ける操作ログ情報受付部、
前記操作ログ情報を用いて、該操作ログ情報における操作内容が、予め定められたアクセス処理であったかを判定し、アクセス処理であったと判定した場合には、該操作ログ情報におけるファイル識別情報とファイルの所在場所とを抽出するアクセス判定部、
前記抽出したファイルの所在場所に該当するコンピュータ端末に対して前記抽出したファイル識別情報を渡すことで、前記ファイル識別情報に対応するファイルが、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部、
前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイ

ル識別情報とを前記コンピュータ端末から受け取ると、前記ファイル識別情報と、前記ファイル識別情報に対応する所在場所とを前記記憶装置に記憶させる監視対象ファイル登録処理部、
`【発明の詳細な説明】を特徴とするファイル管理プログラム。
【技術分野】
【0001】
本発明は、企業などの組織において使用されているコンピュータシステムで、監視対象となる個人情報や機密情報などを含むファイルの所在場所を管理するファイル管理システムに関する。
【背景技術】
【0002】
近年、企業などの組織において使用されているコンピュータシステムからの情報流出が相次いだことから、それを防止することが組織において非常に重要な問題となっている。そのため、企業などの組織では、当該組織で使用しているコンピュータシステムにおける個人情報や機密情報を含むファイルに対する厳重な取り扱いが求められている。
【0003】
一般的に情報流出を防止するためには、個人情報や機密情報を含むファイルは、外部の者のみならず、アクセス権限がない組織内のユーザがそのファイルを取り扱うことができないようにすることが求められる。そのような場合、それらのファイルに対する組織内の各ユーザからのアクセスを監視したり、ユーザによるそれらのファイルに対する不適切な操作がないか、などを操作ログを監視することで対応している。
【0004】
ところが組織で使用しているコンピュータシステムでは、各種のファイルサーバやクライアント端末が多数存在しており、個人情報や機密情報を含むファイルがどのファイルサーバ、クライアント端末に所在するのかが分からないことが多い。そのため、どのファイルを重点的に監視したらよいのかが分からないことから、コンピュータシステムにおいて、個人情報や機密情報を含むファイルがどこに所在するのか、を把握することが求められている。
【0005】
そこで下記特許文献１、特許文献２では、コンピュータシステム上に存在する個人情報を含む多数のファイルを管理するシステムが開示されている。
【0006】
【特許文献1】特開２００６－７９２１６号公報
【特許文献2】特開２００６－７９５８８号公報
【発明の開示】
【発明が解決しようとする課題】
【0007】
特許文献１、特許文献２のシステムでは、コンピュータシステム上に存在するすべてのクライアント端末やファイルサーバにおいて、そこで記憶しているすべてのファイルについて、個人情報を含むファイルであるかを全文検索することで、個人情報を含むファイルの所在を把握している。これによって、個人情報を含むファイルのすべての所在を管理することが出来る点で有益である。
【0008】
しかしこのようなシステムを用いた場合、各クライアント端末やファイルサーバで記憶するすべてのファイルに対して個人情報を含むかを全文検索しているので、各クライアント端末やファイルサーバに対して非常に大きな負荷が発生することとなり、またコンピュータシステム全体でも非常に大きな負荷が発生する。そのため、コンピュータシステム全体のパフォーマンスの低下につながりかねない。
【0009】
そのためコンピュータシステムに出来るだけ負荷をかけずに、情報流出を防止するため

の個人情報や機密情報を含むファイルの所在場所を管理することが求められている。
【課題を解決するための手段】
【0010】
そこで本発明者は、上記問題点に鑑み、コンピュータシステムに出来るだけ負荷をかけないで、必要な個人情報や機密情報を含むファイルの所在場所を管理することが出来るファイル管理システムを発明した。
【0011】
請求項１の発明は、コンピュータシステムで利用されている個人情報または機密情報を含むファイルの所在場所を管理するファイル管理システムであって、前記ファイル管理システムは、監視対象となる個人情報または機密情報を含むファイルの所在場所を記憶する監視対象ファイル記憶部と、前記コンピュータシステムを構成するコンピュータ端末の操作ログ情報を用いて、該操作ログ情報におけるファイルに対してアクセスがあったかを、該操作ログ情報の操作内容により判定するアクセス判定部と、前記アクセスがあったと判定したファイルを記憶するコンピュータ端末に対して、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部と、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果を前記コンピュータ端末から受け取ると、前記ファイルの所在場所を前記監視対象ファイル記憶部に記憶させる監視対象ファイル登録処理部と、を有するファイル管理システムである。
【0012】
本発明のファイル管理システムを用いることによって、個人情報や機密情報を含むファイルの所在場所について、従来よりも大幅に負荷を軽減してその所在場所を管理することが可能となる。それは、従来技術のように、各クライアント端末やファイルサーバで記憶しているすべてのファイルを全文検索して個人情報のファイルであるかを判定するのではなく、本発明では、操作ログ情報を用いて、ユーザによる何らかのアクセスがあったファイルを抽出し、抽出したファイルについて個人情報や機密情報を含むファイルであるか、を判定することで監視対象となるファイルであるかを特定しているためである。
【0013】
つまり個人情報や機密情報の情報流出は、そのファイルに対して何らかのアクセスがあることによって利用価値があるファイル（実際に使用されているファイル）であると考えられ、逆にアクセスがなければそれはたとえ個人情報や機密情報が含まれていても利用価値がないファイル（すでに使用されていないファイル）であると考えられる。これによって、従来のようにすべてのファイルの全文検索を行わずとも、いわば利用価値のあるファイル（つまり情報流出した場合に問題になりそうなファイル）を目星をつけて検索することが出来るので、コンピュータシステムに対する負荷の大幅な軽減を図ることが出来る。
【0014】
請求項２の発明において、前記ファイル管理システムは、更に、各コンピュータ端末の操作ログ情報を記憶する操作ログ情報記憶部と、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果を前記コンピュータ端末から受け取ると、前記ファイルの類似ファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報に基づいて検索する類似ファイル検索部と、を有するファイル管理システムである。
【0015】
本発明のように構成することで、アクセス判定部で判定したファイルだけではなく、そのファイルのファイル識別情報と同一又は類似のファイル識別情報である類似ファイルについても、個人情報や機密情報を含むファイルであるか、を判定することが出来る。
【0016】
請求項３の発明において、前記ファイル管理システムは、更に、各コンピュータ端末の操作ログ情報を記憶する操作ログ情報記憶部と、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果を前記コンピュータ端末から受け取ると、前記ファイルの関連ファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報に基づいて検索する関連ファイル検索部と、を有するファイル管理システムである。

【0017】
本発明のように構成することで、アクセス判定部で判定したファイルだけではなく、そのファイルの内容をコピーなどして関連性のあると考えられるファイル（関連ファイル）についても、個人情報や機密情報を含むファイルであるか、を判定することが出来る。
【0018】
請求項４の発明は、コンピュータシステムで利用されている個人情報または機密情報を含むファイルの所在場所を管理するファイル管理システムであって、前記ファイル管理システムは、監視対象となる個人情報または機密情報を含むファイルのファイル識別情報と所在場所を記憶する監視対象ファイル記憶部と、前記コンピュータシステムを構成する各クライアント端末から操作ログ情報を受け付ける操作ログ情報受付部と、前記操作ログ情報を用いて、該操作ログ情報における操作内容が、予め定められたアクセス処理であったかを判定し、アクセス処理であったと判定した場合には、該操作ログ情報におけるファイル識別情報とファイルの所在場所とを抽出するアクセス判定部と、前記抽出したファイルの所在場所に該当するコンピュータ端末に対して前記抽出したファイル識別情報を渡すことで、前記ファイル識別情報に対応するファイルが、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部と、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、前記ファイル識別情報と、前記ファイル識別情報に対応する所在場所とを前記監視対象ファイル記憶部に記憶させる監視対象ファイル登録処理部と、を有するファイル管理システムである。
【0019】
上述の請求項１の発明は、本発明のように構成することも出来る。本発明のように構成しても、同様の技術的効果を得ることが出来る。
【0020】
請求項５の発明において、前記ファイル管理システムは、更に、前記操作ログ情報受付部で受け付けた操作ログ情報を記憶する操作ログ情報記憶部と、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、そのファイル識別情報に基づいて、同一または類似のファイル識別情報を有するほかのファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報から検索し、前記検索した類似ファイルのファイル識別情報とその所在場所とを該操作ログ情報から抽出する類似ファイル検索部、を有しており、前記検索要求部は、前記類似ファイル検索部が抽出した類似ファイルの所在場所に該当するコンピュータ端末に対して前記抽出した類似ファイルのファイル識別情報を渡すことで、前記類似ファイルが、個人情報または機密情報を含むかの検索を要求する、ファイル管理システムである。
【0021】
本発明のように構成しても、上述の発明と同様に、類似ファイルについて、個人情報や機密情報を含むファイルであるか、を判定することが出来る。
【0022】
請求項６の発明において、前記ファイル管理システムは、更に、前記操作ログ情報受付部で受け付けた操作ログ情報を記憶する操作ログ情報記憶部と、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、そのファイル識別情報に対応するファイルに関連するほかのファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報から検索し、前記検索した関連ファイルのファイル識別情報とその所在場所とを該操作ログ情報から抽出する関連ファイル検索部、を有しており、前記検索要求部は、前記関連ファイル検索部が抽出した関連ファイルの所在場所に該当するコンピュータ端末に対して前記抽出した関連ファイルのファイル識別情報を渡すことで、前記関連ファイルが、個人情報または機密情報を含むかの検索を要求する、ファイル管理システムである。
【0023】

本発明のように構成しても、上述の発明と同様に、関連ファイルについて、個人情報や機密情報を含むファイルであるか、を判定することが出来る。

【0024】

請求項７の発明において、前記ファイル管理システムは、更に、前記コンピュータシステムにおいて使用されているファイルのファイル識別情報とその所在場所とを記憶するファイルインデックス記憶部と、前記操作ログ情報受付部で受け付けた操作ログ情報の操作内容に基づいて、ファイルに対して、追加、変更、削除のいずれかがされたかを判定し、判定した場合には、該ファイルの操作ログ情報におけるファイル識別情報または所在場所に基づいて、前記ファイルインデックス記憶部のファイル識別情報及び／又は所在場所を更新するファイルインデックス処理部と、前記操作ログ情報受付部で受け付けた操作ログ情報を記憶する操作ログ情報記憶部と、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、そのファイル識別情報に基づいて、同一または類似のファイル識別情報を有するほかのファイルが存在するかを、前記ファイルインデックス記憶部に記憶するファイル識別情報から検索し、前記検索した類似ファイルの所在場所を前記ファイルインデックス記憶部から抽出する類似ファイル検索部と、を有しており、前記検索要求部は、前記類似ファイル検索部が抽出した類似ファイルの所在場所に該当するコンピュータ端末に対して前記抽出した類似ファイルのファイル識別情報を渡すことで、前記類似ファイルが、個人情報または機密情報を含むかの検索を要求する、ファイル管理システムである。

【0025】

上述の発明において、ファイルインデックスを用いてファイル管理を行っても良い。ファイルインデックスを用いて最新の所在場所を管理しておくことによって、常に最新の場所を管理しているので、それに基づいて、適切なファイル所在場所の管理が可能となる。そして、ファイルインデックスを用いた場合に類似ファイル検索を行うのは、本発明のように構成することが好ましい。

【0026】

請求項８の発明において、前記ファイル管理システムは、更に、前記コンピュータシステムにおいて使用されているファイルのファイル識別情報とその所在場所とを記憶するファイルインデックス記憶部と、前記操作ログ情報受付部で受け付けた操作ログ情報の操作内容に基づいて、ファイルに対して、追加、変更、削除のいずれかがされたかを判定し、判定した場合には、該ファイルの操作ログ情報におけるファイル識別情報または所在場所に基づいて、前記ファイルインデックス記憶部のファイル識別情報及び／又は所在場所を更新するファイルインデックス処理部と、前記操作ログ情報受付部で受け付けた操作ログ情報を記憶する操作ログ情報記憶部と、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、そのファイル識別情報に対応するファイルに関連するほかのファイルが存在するかを、前記操作ログ情報記憶部に記憶する操作ログ情報から検索し、前記検索した関連ファイルのファイル識別情報を該操作ログ情報から抽出し、抽出した関連ファイルのファイル識別情報に対応する所在場所を前記ファイルインデックス記憶部から抽出する関連ファイル検索部と、を有しており、前記検索要求部は、前記関連ファイル検索部が抽出した関連ファイルの所在場所に該当するコンピュータ端末に対して前記抽出した関連ファイルのファイル識別情報を渡すことで、前記関連ファイルが、個人情報または機密情報を含むかの検索を要求する、ファイル管理システムである。

【0027】

上述の発明において、ファイルインデックスを用いてファイル管理を行っても良い。ファイルインデックスを用いて最新の所在場所を管理しておくことによって、常に最新の場所を管理しているので、それに基づいて、適切なファイル所在場所の管理が可能となる。そして、ファイルインデックスを用いた場合に関連ファイル検索を行うのは、本発明のように構成することが好ましい。

【0028】

請求項９の発明において、前記ファイル管理システムは、更に、前記監視対象ファイル記憶部に記憶したファイル所在場所のファイルに対する操作ログ情報を監視する監視処理部、を有するファイル管理システムである。

【0029】

監視対象となったファイルについては、本発明のように監視対象ファイル記憶部に記憶したファイル所在場所に基づいて実行するが、その監視処理をファイル管理システムで備えても良い。

【0030】

請求項１０の発明は、監視対象となる個人情報または機密情報を含むファイルの所在場所を記憶する記憶装置を有するコンピュータ端末を、コンピュータシステムを構成するコンピュータ端末の操作ログ情報を用いて、該操作ログ情報におけるファイルに対してアクセスがあったかを、該操作ログ情報の操作内容により判定するアクセス判定部、前記アクセスがあったと判定したファイルを記憶するコンピュータ端末に対して、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果を前記コンピュータ端末から受け取ると、前記ファイルの所在場所を前記記憶装置に記憶させる監視対象ファイル登録処理部、として機能させるファイル管理プログラムである。

【0031】

請求項１１の発明は、監視対象となる個人情報または機密情報を含むファイルのファイル識別情報と所在場所を記憶する記憶装置を有するコンピュータ端末を、コンピュータシステムを構成する各クライアント端末から操作ログ情報を受け付ける操作ログ情報受付部、前記操作ログ情報を用いて、該操作ログ情報における操作内容が、予め定められたアクセス処理であったかを判定し、アクセス処理であったと判定した場合には、該操作ログ情報におけるファイル識別情報とファイルの所在場所とを抽出するアクセス判定部、前記抽出したファイルの所在場所に該当するコンピュータ端末に対して前記抽出したファイル識別情報を渡すことで、前記ファイル識別情報に対応するファイルが、個人情報または機密情報を含むファイルであるかの検索を要求する検索要求部、前記ファイルが個人情報または機密情報を含むファイルであるとの検索結果と前記ファイル識別情報とを前記コンピュータ端末から受け取ると、前記ファイル識別情報と、前記ファイル識別情報に対応する所在場所とを前記記憶装置に記憶させる監視対象ファイル登録処理部、として機能させるファイル管理プログラムである。

【0032】

これらのファイル管理プログラムを所定のコンピュータ端末（例えば管理サーバ）に読み込ませて実行することで、上述のファイル管理システムを実現できる。

【発明の効果】

【0033】

本発明のファイル管理システムを用いることによって、コンピュータシステムに出来るだけ負荷をかけないで、必要な個人情報や機密情報を含むファイルの所在を管理することが出来る。

【発明を実施するための最良の形態】

【0034】

本発明のファイル管理システム１の全体の概念図を図１に示す。また本発明のファイル管理システム１の一実施例のシステム構成の概念図を図２に示す。

【0035】

管理サーバ２、ファイルサーバ３、クライアント端末４は通常のコンピュータ端末（サーバも含む）が備えるべき通常のハードウェア構成を適宜備えている。また管理サーバ２、ファイルサーバ３、クライアント端末４には所定のプログラムが読み込まれ、処理されることにより実現される。管理サーバ２は、複数のクライアント端末４においてどのようなプログラムや操作が実行されているのか、を保存、監視する。従って、各クライアント端末４には、当該クライアント端末４において実行されているプログラム名、ファイル名

などのファイル識別情報や、当該クライアント端末４の入力装置で入力された情報、クライアント端末４における処理や操作などがリアルタイムで、或いは定期的に、あるいは新たなプログラムやファイルが実行された場合または終了した場合などの所定のタイミングでクライアント端末４から管理サーバ２にその操作ログの情報を送信する機能を備えている。操作ログを送信する機能は、クライアント端末４の演算装置で実行しているプログラム名やファイル名を抽出したり、メモリ内のプログラム名やファイル名を抽出したり、当該クライアント端末４の入力装置で入力された、あるいは操作された情報などを送信すればよい。

【0036】

またクライアント端末４やファイルサーバ３や所定のサーバには、管理サーバ２からの検索要求を受け付けることによって、検索要求の際に受け付けたファイル識別情報に基づき、当該ファイル識別情報に対応するファイルに個人情報、機密情報が含まれているかを検索する機能（検索処理部（図示せず））が備えられている。検索処理部は、検索要求で受け付けたファイル識別情報のファイルに、住所、氏名、電話番号、電子メールアドレス、役職、生年月日などの個人情報が含まれているか、特定のキーワードに相当する機密情報が含まれているか、を検索する。そして検索結果として、ファイル識別情報と共に、個人情報や機密情報を含むファイルである、または個人情報や機密情報を含むファイルではない、ことを返す。

【0037】

個人情報の検索は、住所や電話番号、電子メールアドレス、生年月日特有の文字・数字・記号などの配列などから個人情報であるか否かを判定することが出来る。例えば住所であれば、都道府県名、市町村名などの順番で配置されているので、それらの名称を記憶する保存部を管理サーバ２やクライアント端末４、或いは所定のサーバ上に記憶しておき、検索処理部がファイル検索の際に、その保存部に記憶する情報との一致性を判定することで行える。また電話番号は数字が所定の桁数で並んでいれば（記号「－」が所定の桁に位置していることを判定しても良い）電話番号であると判定でき、また電子メールアドレスは英数字と「＠」を含み、その最後が「co.jp」、「com」、「ac.jp」などの所定の英字列になっていれば電子メールアドレスであると判定でき、更に、生年月日は、元号の後に所定桁数の数字または２桁か４桁の数字があり、その後、「年」、所定桁数の数字、「月」、所定桁数の数字、「日」と並んでいれば生年月日であると判定できる。

【0038】

このようにして判定した個人情報が、当該検索対象となったファイルにどれだけ含まれているか、で個人情報のファイルであるかどうかを判定する。所定数以上含まれていれば個人情報を含むファイルであると判定する。

【0039】

また機密情報を含むファイルの検索の際には、上述の管理サーバ２やクライアント端末４、或いは所定のサーバ上に記憶している保存部に、機密情報に該当するキーワードが予め記憶されており、検索処理部がファイル検索の際に、その保存部に記憶するキーワードとの一致性を判定することで行える。機密情報に該当するキーワードとしては、例えば、社員名、新商品名、開発中の新機能の名前、業務提携先の企業名などの予め設定された情報や、秘密、極秘、シークレットなど機密を意味する用語などがある。図５に機密情報を記憶する保存部を模式的に示す。

【0040】

管理サーバ２、ファイルサーバ３、クライアント端末４は、プログラムの演算処理を実行するＣＰＵなどの演算装置と、情報を記憶するＲＡＭやハードディスクなどの記憶装置と、演算装置の処理結果や記憶する情報をインターネットやＬＡＮなどのネットワークを介して送受信する通信装置と、を少なくとも有している。コンピュータ上で実現する各機能（各手段）は、その処理を実行する手段（プログラムやモジュールなど）が演算装置に読み込まれることでその処理が実行される。各機能は、記憶装置に記憶した情報をその処理において使用する場合には、該当する情報を当該記憶装置から読み出し、読み出した情

報を適宜、演算装置における処理に用いる。当該管理サーバ２、ファイルサーバ３、クライアント端末４には、キーボードやマウスやテンキーなどの入力装置、ディスプレイなどの表示装置を有していても良い。図３にこれらのハードウェア構成の一例を模式的に示す。

【0041】

本発明における各手段は、その機能が論理的に区別されているのみであって、物理上あるいは事実上は同一の領域を為していても良い。

【実施例】

【0042】

図２に示すファイル管理システム１の管理サーバ２は、操作ログ情報受付部５と操作ログ情報記憶部６とアクセス判定部７と検索要求部８と監視対象ファイル登録処理部９と監視対象ファイル記憶部１０と類似ファイル検索部１１と関連ファイル検索部１２と監視処理部１３とを有する。

【0043】

操作ログ情報受付部５は、各クライアント端末４から、好ましくはリアルタイムで、または定期的にあるいは不定期に、当該クライアント端末４における操作ログ情報を受け取る。受け取った操作ログ情報は、後述する操作ログ情報記憶部６に記憶する。また操作ログ情報としては、各クライアント端末４における操作内容を示す情報（例えば「データコピー」、「ファイル選択」、「ドライブ追加」など）と、その操作対象となったファイル名（「ファイル識別情報」。なおファイル識別情報にはファイル名などのほかに、ファイルを識別できる情報であれば如何なるものでもよく、ＩＤなどでも良い）やアプリケーション名（「アプリケーション識別情報」。なおアプリケーション識別情報にはアプリケーション名などのほかに、アプリケーションを識別できる情報であれば如何なるものでもよく、ＩＤなどでも良い）、ファイルやアプリケーションの所在場所を示す情報、日時、コンピュータ名（コンピュータ識別情報はコンピュータを識別できる情報であれば如何なるものでもよく、ＩＤなどでも良い）、ログイン名などが含まれていることが好ましい。操作ログ情報の一例を図６に示す。

【0044】

操作ログ情報記憶部６は、操作ログ情報受付部５が各クライアント端末４から受け取った操作ログ情報を記憶する。図７に操作ログ情報記憶部６の一例を示す。

【0045】

アクセス判定部７は、リアルタイムで（例えば操作ログ情報受付部５で操作ログ情報を受け付けたタイミングで）、定期的にまたは不定期に、操作ログ情報記憶部６に記憶した操作ログ情報について、操作内容としてファイルへの所定のアクセス処理をした操作ログ情報が含まれているかを判定する。ファイルへの所定のアクセス処理とは、ファイルの起動、ファイルを編集、コピー、移動、閲覧などが例としてあり、ファイルに対する何らかの操作が含まれる。アクセス処理として上述が設定されており、操作ログ情報が図７の場合、「ファイル起動」を操作内容に含む２つの操作ログ情報が、ファイルへのアクセスがあった操作ログ情報として判定できる。これを模式的に示すのが図８である。

【0046】

アクセス判定部７は、所定のアクセス処理を操作内容として含む操作ログ情報を操作ログ情報記憶部６から抽出すると、抽出した操作ログ情報に含まれるファイル識別情報とその所在場所とを抽出する。図８の場合、ファイル識別情報として「顧客情報一覧表」、ファイルの所在場所として「ファイルサーバ３「Ｔｏｋｙｏ－ｆｓ」の「重要書類¥顧客」」と、ファイル識別情報として「一般公開プレゼン資料」、ファイルの所在場所として「ファイルサーバ３「Ｔｏｋｙｏ－ｆｓ」の「公開用¥資料」」を抽出する。なおファイルの所在場所がファイルサーバ３や所定のサーバでない場合、つまり特定のクライアント端末４の場合には、ファイルの所在場所として「クライアント端末名（クライアント端末識別情報）」が含まれていればそれを抽出し、含まれていなければ、操作ログ情報に含まれるクライアント端末名（クライアント端末識別情報）を抽出することで、ファイルを記憶

するクライアント端末４を抽出できる。

【0047】

検索要求部８は、アクセス判定部７で抽出したファイルを記憶するファイルサーバ３やクライアント端末４、所定のサーバなどに対して、当該ファイル識別情報と、当該ファイルが個人情報や機密情報を含んでいるかの検索要求を渡す。図８の場合、ファイルサーバ「Ｔｏｋｙｏ－ｆｓ」に対して、「顧客情報一覧表」と「一般公開プレゼン資料」の検索要求を渡す。この検索要求とファイル識別情報とを受け取ったファイルサーバ３やクライアント端末４、所定のサーバなどは、そこに備える検索処理部で当該ファイルに対して個人情報や機密情報を含んでいるかの検索処理を実行する。検索処理は上述のように行える。

【0048】

また検索要求部８は、後述する類似ファイル検索部１１、関連ファイル検索部１２でファイル識別情報とその所在場所を抽出すると、当該ファイルを記憶するファイルサーバ３やクライアント端末４、所定のサーバなどに対して、当該ファイル識別情報と、当該ファイルが個人情報や機密情報を含んでいるかの検索要求を渡し、個人情報や機密情報の検索処理を実行させる。なおこの検索処理も上述と同様である。

【0049】

監視対象ファイル登録処理部９は、検索要求部８における検索要求の結果、当該検索を行ったファイルサーバ３、クライアント端末４、所定のサーバなどから、個人情報や機密情報を含むファイルであることの検索結果を受け取ると、その検索対象となったファイルは監視対象となるファイルであることが分かるので、そのファイルのファイル識別情報と所在場所とを、後述する監視対象ファイル記憶部１０に記憶する。なお個人情報や機密情報を含むファイルではないことの検索結果を受け取ると、そのファイルに対するファイル識別情報や、ファイルの所在場所を示す情報、日時、クライアント端末識別情報、ログイン名などは削除することが好ましい。

【0050】

監視対象ファイル記憶部１０は、コンピュータシステムの所定の管理者が、個人情報や機密情報が含まれているファイルであるとして、操作ログ情報の追跡などの監視対象とするファイルのリストを記憶する。図９に監視対象ファイル記憶部１０の一例を模式的に示す。図９の監視対象ファイル記憶部１０では、監視対象であると判定されたファイルのファイル識別情報と所在場所とを記憶している。

【0051】

類似ファイル検索部１１は、監視対象ファイル登録処理部９で、検索要求部８における検索要求の結果、当該検索を行ったファイルサーバ３、クライアント端末４、所定のサーバなどから、個人情報や機密情報を含むファイルであることの検索結果を受け取ったファイルについて、それと同一または類似するファイル識別情報を有するファイル（類似ファイル）が存在するか、を操作ログ情報記憶部６から検索する（この検索の際に、操作ログ情報記憶部６に記憶する操作ログ情報のすべてを検索対象としても良いし、所定期間内の操作ログ情報を検索対象としても良い）。これは個人情報や機密情報を含むファイル識別情報と同一または類似のファイル識別情報を有している類似ファイルであれば、そのファイルも同じく個人情報や機密情報を含むファイルである可能性が高いからである。

【0052】

類似ファイルのファイル識別情報の検索は、監視対象ファイル登録処理部９で受け取ったファイル識別情報と同一または類似のファイル識別情報が存在するかを操作ログ情報記憶部６から検索すればよい。例えば監視対象ファイル登録処理部９で受け取ったファイル識別情報が「顧客情報一覧表」であり、操作ログ情報記憶部６が図１０の場合、それに類似するファイル識別情報として、「お客様情報一覧表」がある。従って、このファイルのファイル識別情報（「お客様情報一覧表」）と所在場所（クライアント端末識別情報「ＤＥＦ４５６７８９１２３」と「Ｃ：¥Documents and Settings¥デスクトップ」）とを抽出し、それを当該ファイルを記憶するファイルサーバ３や所定のサーバ、クライアント端

末４の検索要求部８に渡すことで（この場合はクライアント端末識別情報「ＤＥＦ４５６７８９１２３」の検索要求部８に渡す）、同一または類似のファイル識別情報を有する類似ファイルに対して、個人情報や機密情報が含まれているファイルであるかの検索処理を実行させることが出来る。

【0053】

また類似するファイル識別情報であるかは、管理サーバ２や所定のサーバに類義語データベースのような記憶部を備えておき、それを用いて公知の類義語検索を実行することで、検索可能である。

【0054】

類似ファイルの判定には上述のようにファイル識別情報の類義語検索を行うほか、次のような方法もある。すなわち、個人情報や機密情報を含むファイルのファイル識別情報と、操作ログ情報記憶部６の操作ログ情報におけるファイル識別情報やファイルインデックス記憶部１５（後述）におけるファイル識別情報との、一致度を判定し、その一致度が所定値以上であればそのファイルについても類似ファイルであると判定する。例えば、個人情報や機密情報を含むファイルとして判定したファイルのファイル識別情報が「お客様情報一覧表」であり、操作ログ情報記憶部６に記憶したある操作ログ情報におけるファイル識別情報が「顧客情報一覧表」であった場合、それらの一致度は、８文字中５文字が一致していることから６２．５％となる。そしてこの一致度を所定値と比較して、所定値以上であれば、「顧客情報一覧表」も類似ファイルであると判定し、所定値未満であれば「顧客情報一覧表」は類似ファイルではないと判定する。

【0055】

関連ファイル検索部１２は、監視対象ファイル登録処理部９で、検索要求部８における検索要求の結果、当該検索を行ったファイルサーバ３、クライアント端末４、所定のサーバなどから、個人情報や機密情報を含むファイルであることの検索結果を受け取ったファイルについて、そのファイルに関連するファイル（関連ファイル）が存在するか、を操作ログ情報記憶部６から検索する。ここで関連するファイルとは、ファイルの内容がコピーされたり、貼り付けされたり、その名称（ファイル識別情報など）が変更されたなどの、ファイルに対して所定の操作（関連操作）が行われているファイルをいう。

【0056】

例えば、監視対象ファイル登録処理部９で、検索要求部８における検索要求の結果、当該検索を行ったファイルサーバ３、クライアント端末４、所定のサーバなどから、個人情報や機密情報を含むファイルであることの検索結果を受け取ったファイルのファイル識別情報が「顧客情報一覧表」であって、操作ログ情報記憶部６が図１１であり、関連操作として、「データコピー」、「貼り付け」、「ファイル名の変更」が指定されている場合、まず検索結果を受け取ったファイルに対する操作ログ情報の操作内容に、関連操作が含まれているかを判定し、含まれている場合には、それに対応する操作内容（これは関連操作に予め対応づけて記憶されている）を含む操作ログ情報を検索する。

【0057】

図１１の場合、「顧客情報一覧表」に対して操作内容「データコピー」があり、これは関連操作であるので、「顧客情報一覧表」には関連操作があると判定する。そしてその操作内容は「データコピー」であることから、対応する操作は「貼り付け」操作である。そのため、その操作内容を含む操作ログ情報を検索する。一般的には操作内容「データコピー」のあとの操作ログ情報であって、最初に操作内容「貼り付け」を含む操作ログ情報を、予め定められた対応する操作ログ情報として判定し、その操作ログ情報におけるファイルを関連ファイルとして判定すればよい。上述の場合、「顧客情報一覧表」の「データコピー」の操作ログ情報以降であって、操作内容「貼り付け」を最初に含む操作ログ情報のファイル識別情報は「お客様情報一覧表」である。従って、関連ファイルのファイル識別情報として「お客様情報一覧表」と、その所在場所のクライアント端末識別情報として「ＤＥＦ４５６７８９１２３」「Ｃ：¥Documents and Settings¥デスクトップ」を抽出する。そして抽出した関連ファイルのファイル識別情報「お客様情報一覧表」を、そのファ

イルを記憶するファイルサーバ３や所定のサーバ、クライアント端末４の検索要求部８に渡すことで（この場合はクライアント端末識別情報「ＤＥＦ４５６７８９１２３」の検索要求部８に渡す）、関連ファイルに対して、個人情報や機密情報が含まれているファイルであるかの検索処理を実行させることが出来る。

【0058】

また操作内容として「ファイル名の変更」が行われている場合には、操作ログ情報における操作内容から「ファイル名の変更」を判定すると、当該操作ログ情報におけるファイル識別情報を抽出する。ここで抽出されたファイル識別情報は、一般的には変更前のファイル識別情報なので、変更された後のファイル識別情報（ファイル名）を改めてクライアント端末３から取得する。なお変更後のファイル識別情報（ファイル名）を取得するのは如何なるタイミングでも良く、操作ログ情報をクライアント端末４から受け取った際であっても良い。このように関連ファイル検索部１２は、「ファイル名の変更」を判定した操作ログ情報のファイル識別情報が新たなファイル識別情報に変更されていることが判定できるので、その変更後のファイル識別情報のファイルも関連ファイルであると判定できる。従って関連ファイル検索部１２は前記「ファイル名の変更」を判定した操作ログ情報における所在場所の情報を抽出し、抽出した所在場所のファイルサーバ３や所定のサーバ、クライアント端末４など、当該ファイルを記憶するコンピュータ端末に対して、検索要求部８が、変更後のファイル識別情報を渡すことで、関連ファイルに対して、個人情報や機密情報が含まれているファイルであるかの検索処理を実行させることもできる。

【0059】

なお一般的にはアクセス判定部７で判定した操作ログ情報におけるファイルに対する検索要求の結果、個人情報や機密情報を含むファイルであるとの検索結果を受け取ったファイルに対して、類似ファイル検索部１１における類似ファイル検索処理、関連ファイル検索部１２における関連ファイル検索処理を実行することが好ましいが、類似ファイル、関連ファイルに対する検索要求の結果、個人情報や機密情報を含むファイルであるとの検索結果を受け取ったファイルに対してさらなる類似ファイル検索部１１における類似ファイル検索処理、関連ファイル検索部１２における関連ファイル検索処理を実行しても良い。

【0060】

なお類似ファイル検索部１１、関連ファイル検索部１２は、類似ファイルや関連ファイルを操作ログ情報から検索できなければ、検索要求部８にファイル識別情報などを渡さなくて良い。

【0061】

監視処理部１３は、操作ログ情報を用いて、監視対象ファイル記憶部１０に記憶した監視対象となったファイルについて、所定の操作が行われた場合に、通知や操作制御指示を行う。例えば操作ログ情報を各クライアント端末４から操作ログ情報受付部５で受け付けた場合、監視処理部１３は、その操作ログ情報におけるファイル識別情報と操作内容とを抽出し、監視対象ファイル記憶部１０に含まれるファイル識別情報であると監視対象のファイルであることが判定できるので、その操作内容が所定の操作であるかを判定する。そして所定の操作であった場合に、例えば所定の管理者が利用する管理者端末に対して通知を行ったり、当該操作を行ったクライアント端末４に対して（操作ログ情報のクライアント端末４識別情報から判定可能である）、操作制御指示（例えばコピー不可の制御、クリップボードのデータを消去する制御などの指示）を送信し、当該クライアント端末４で操作制御を行わせる。

【0062】

例えば、監視対象ファイルを起動、移動、編集させたりした場合に、管理者端末に対してアラート通知が行われたり、コピーした場合に、クリップボードのデータを消去する制御指示を当該クライアント端末４に送信する。

【0063】

次に本発明の処理プロセスの一例を図４のフローチャート、図２のシステム構成の概念図を用いて説明する。

【0064】
各クライアント端末４は管理サーバ２に対して、リアルタイムで、或いは定期的にまたは不定期に操作ログ情報を送信しており、その操作ログ情報を操作ログ情報受付部５は受け付ける（Ｓ１００）。操作ログ情報受付部５で受け付けた操作ログ情報は、操作ログ情報記憶部６に保存する（Ｓ１１０）。この際に、操作ログ情報は、クライアント端末識別情報ごと、ログイン名（ユーザ名）ごとに保存することが好ましい。
【0065】
そして所定のタイミングで、アクセス判定部７は、操作ログ情報記憶部６に記憶した操作ログ情報（または操作ログ情報受付部５で受け付けた操作ログ情報）について、操作内容として、ファイルへの所定のアクセス処理をした操作ログ情報が含まれているかを判定する（Ｓ１２０）。すなわち操作ログ情報の操作内容として、「ファイルの起動」、「ファイルを編集」、「コピー」、「移動」、「閲覧」などを含む操作ログ情報を判定する。
【0066】
このようにしてアクセス判定部７は、アクセス処理を操作内容として含む操作ログ情報のファイル識別情報とファイルの所在場所とを抽出する。そして抽出したファイル識別情報がすでに監視対象ファイル記憶部１０に登録されているかを確認し（Ｓ１３０）、監視対象ファイルとして登録されていなければ、抽出したファイル所在場所のファイルサーバ３、所定のサーバ、クライアント端末４に対して、当該ファイル識別情報を渡すことで、当該ファイルが個人情報や機密情報を含むファイルであるかの検索要求を検索要求部８が行う。この検索要求を受けた、当該ファイルを記憶するファイルサーバ３、所定のサーバ、クライアント端末４は、検索処理部で、当該ファイル識別情報を有するファイルに、個人情報や機密情報を含んでいるかを検索し（Ｓ１４０）、その結果を管理サーバ２に返す（Ｓ１５０）。
【0067】
一方、Ｓ１３０において、抽出したファイル識別情報がすでに監視対象ファイル記憶部１０に登録されている場合には、抽出したファイル識別情報の類似ファイル、関連ファイルの検索処理を実行する。すなわちＳ１７０以降の処理を実行することとなる。
【0068】
Ｓ１５０における検索結果として、前記抽出したファイル識別情報のファイルが、個人情報や機密情報を含んでいるファイルであることを受け取ると、監視対象ファイル登録処理部９は、新たに監視対象ファイルとして、そのファイル識別情報と所在場所とを監視対象ファイル記憶部１０に記憶する（Ｓ１６０）。なおこの登録の前に、再度、監視対象ファイル記憶部１０に当該ファイル識別情報が登録されていないかの重複チェックを行っても良い。またＳ１３０における登録チェックや重複チェックの際には、同一のファイル識別情報を異なるクライアント端末４やファイルサーバ３などで使用していることが考えられるので、ファイル識別情報のみならず、ファイルの所在場所も検索キーとして使用して検索することが好ましい。つまりファイル識別情報と所在場所とが一致した場合には、すでに登録されているファイルと判定し、そうでなければ新たに監視対象ファイルとして追加すればよい。
【0069】
また検索結果として、個人情報や機密情報を含んでいるファイルであることを受け取ると、類似ファイル検索部１１が類似ファイル検索を操作ログ情報記憶部６で実行し、また関連ファイル検索部１２が関連ファイル検索を操作ログ情報記憶部６で実行する（Ｓ１７０）。そして類似ファイル、関連ファイルが検索できたら、類似ファイル検索部１１、関連ファイル検索部１２は、その類似ファイル、関連ファイルの各ファイル識別情報がすでに監視対象ファイル記憶部１０に登録されているかを確認し（Ｓ１８０）、それらが監視対象ファイルとして登録されていなければ、検索要求部８が、検索した類似ファイル、関連ファイルの所在場所であるファイルサーバ３、クライアント端末４、所定のサーバに対して、類似ファイル、関連ファイルのファイル識別情報を渡すことで、当該ファイルが個人情報や機密情報を含むファイルであるかの検索要求を行う。この検索要求を受けた、当

該ファイルを記憶するファイルサーバ３、所定のサーバ、クライアント端末４は、検索処理部で、当該ファイル識別情報を有するファイルに、個人情報や機密情報を含んでいるかを検索し（Ｓ１９０）、その結果を管理サーバ２に返す（Ｓ２００）。

【0070】

一方、Ｓ１８０において、類似ファイル、関連ファイルとして検索した各ファイル識別情報がすでに監視対象ファイル記憶部１０に登録されている場合には、そのままＳ２２０以降の処理を実行する。

【0071】

このようにして類似ファイル、関連ファイルについての検索結果を監視対象ファイル登録処理部９で受け取ると、新たに監視対象ファイルとして、そのファイル識別情報と所在場所とを監視対象ファイル記憶部１０に記憶する（Ｓ２１０）。なおこの登録の前に、再度、監視対象ファイル記憶部１０に当該ファイル識別情報が登録されていないかの重複チェックを行っても良い。

【0072】

なおＳ１７０からＳ２１０までの処理を、更に類似ファイル、関連ファイルについての検索結果に対して行っても良い。また類似ファイル、関連ファイルの検索処理は、どちらを先に行っても良いし、並列して行っても良い。

【0073】

このようにして監視対象ファイル記憶部１０に、監視対象のファイルとして記憶されたファイルについて、監視処理部１３は、操作ログ情報を用いて監視を実行する（Ｓ２２０）。

【0074】

また監視処理部１３における監視処理は、常に行われていることが好ましい。

【実施例】

【0075】

上述の実施例１の処理について、更に、組織のコンピュータシステムにおいて使用されているファイルのファイル識別情報とその現在の所在場所とを対応づけて記憶するファイルインデックス記憶部１５を用いても同様の処理を実行できる。実施例１の場合、操作ログ情報記憶部６に記憶した操作ログ情報を用いて類似ファイル検索、関連ファイル検索を行っているので、類似ファイル、関連ファイルとして検索したファイルの所在場所が変更している場合もある。従って、ファイルインデックス記憶部１５を参照することによって、的確な検索処理を実行するように構成しても良い。なおファイルインデックス記憶部１５を用いる場合には、各クライアント端末４、ファイルサーバ３、所定のサーバで用いるファイルのファイル識別情報は重複しないことが好ましいが、重複してもファイル識別情報に自動的にひもづけられている情報（例えばファイルの作成場所などの情報）に基づいて、ファイルを一意に特定できることがよい。なおファイル識別情報には、ファイル識別情報に自動的にひもづけられている情報も含まれる。

【0076】

本実施例における管理サーバ２は、操作ログ情報受付部５、操作ログ情報記憶部６、アクセス判定部７、監視対象ファイル登録処理部９、監視対象ファイル記憶部１０、類似ファイル検索部１１、関連ファイル検索部１２、監視処理部１３、ファイルインデックス処理部１４、ファイルインデックス記憶部１５とを有する。図１２に本実施例におけるファイル管理システム１のシステム構成の一例を模式的に示す。

【0077】

ファイルインデックス処理部１４は、操作ログ情報受付部５で受け付けた操作ログ情報に基づいて、各クライアント端末４、ファイルサーバ３、所定のサーバなどのコンピュータシステムで使用されたファイルの一覧を、ファイル識別情報とその所在場所とを対応づけて、後述するファイルインデックス記憶部１５に記憶させる。またファイルインデックス記憶部１５のファイル識別情報と所在場所とを最新の情報に更新する。

【0078】

またファイルインデックス処理部１４は、操作ログ情報受付部５で受け付けた操作ログ情報のうち、所定の操作内容を含む操作ログ情報、例えばファイルの作成、ファイルの名前変更、移動、削除などの操作内容を含む操作ログ情報を判定すると、その操作内容に基づいて、ファイルインデックス記憶部１５に記憶するファイルの一覧を更新する。

【0079】

例えば、操作内容が「ファイルの作成」である操作ログ情報を受け取ると、その操作ログ情報におけるファイル識別情報と所在場所とを抽出し、新たなファイルとしてファイルインデックス記憶部１５にそのファイル識別情報と所在場所とを記憶する。

【0080】

操作内容が「ファイルの名前変更」である操作ログ情報を受け取ると（この場合、変更後のファイル識別情報も受け取っている）、その操作ログ情報におけるファイル識別情報（変更前のファイル識別情報）と所在場所とを抽出し、対応するファイル識別情報（変更前のファイル識別情報）と所在場所とをファイルインデックス記憶部１５から抽出する。そして抽出したファイル識別情報を新たなファイル識別情報（変更後のファイル識別情報）で更新してファイルインデックス記憶部１５を更新する。

【0081】

また操作内容が「移動」である操作ログ情報を受け取ると（この場合、変更後の所在場所も受け取っている）、その操作ログ情報におけるファイル識別情報と所在場所（変更前の所在場所）とを抽出し、対応するファイル識別情報と所在場所（変更前の所在場所）とをファイルインデックス記憶部１５から抽出する。そして抽出した所在場所を新たな所在場所（変更後の所在場所）で更新してファイルインデックス記憶部１５を更新する。

【0082】

また「削除」である操作ログ情報を受け取ると、その操作ログ情報におけるファイル識別情報と所在場所とを抽出し、対応するファイル識別情報と所在場所とをファイルインデックス記憶部１５から抽出する。そして抽出したファイル識別情報と所在場所とをファイルインデックス記憶部１５から削除することによって、更新する。

【0083】

なおファイルインデックス処理部１４における処理は、如何なるタイミングで行っても良いが、好ましくは操作ログ情報受付部５で操作ログ情報を受け付けた段階、あるいは検索要求部８における処理よりも前のいずれかの段階で行う。

【0084】

ファイルインデックス記憶部１５は、各クライアント端末４、ファイルサーバ３、所定のサーバなどのコンピュータシステムで使用されたファイルの一覧を、ファイル識別情報とその現在の所在場所とを対応づけて記憶する。図１３にファイルインデックス記憶部１５の一例を模式的に示す。

【0085】

類似ファイル検索部１１は、監視対象ファイル登録処理部９で、検索要求部８における検索要求の結果、当該検索を行ったファイルサーバ３、クライアント端末４、所定のサーバなどから、個人情報や機密情報を含むファイルであることの検索結果を受け取ったファイルについて、それと同一または類似するファイル識別情報を有するファイル（類似ファイル）が存在するか、をファイルインデックス記憶部１５から検索する。これは個人情報や機密情報を含むファイル識別情報と同一または類似のファイル識別情報を有している類似ファイルであれば、そのファイルも同じく個人情報や機密情報を含むファイルである可能性が高いからである。なお類似ファイルの検索処理は、実施例１と同様である。

【0086】

関連ファイル検索部１２は、実施例１と同様に、関連ファイルが存在するかを操作ログ情報記憶部６から検索するが、検索した関連ファイルについてはそのファイル識別情報を操作ログ情報記憶部６から検索するのみで、当該ファイル識別情報に対応するファイルの所在位置は、ファイルインデックス記憶部１５を参照することにより取得する。

【0087】

なお管理サーバ２におけるほかの機能は、実施例１と同様であるので、説明を省略する。

【0088】

次に本実施例２におけるファイル管理システム１の処理プロセスの一例を図４のフローチャートと図１２の概念図を用いて説明する。

【0089】

各クライアント端末４は管理サーバ２に対して、リアルタイムで、或いは定期的にまたは不定期に操作ログ情報を送信しており、その操作ログ情報を操作ログ情報受付部５は受け付ける（Ｓ１００）。操作ログ情報受付部５で受け付けた操作ログ情報は、操作ログ情報記憶部６に保存する（Ｓ１１０）。この際に、操作ログ情報は、クライアント端末識別情報ごと、ログイン名（ユーザ名）ごとに保存することが好ましい。

【0090】

またＳ１００で操作ログ情報を操作ログ情報受付部５で受け付けると、ファイルインデックス処理部１４は、受け付けた操作ログ情報を用いて、ファイルインデックス記憶部１５に記憶するファイル識別情報と所在場所とを最新の情報に更新する。すなわち操作ログ情報における操作内容として「ファイルの作成」があれば、そのファイル識別情報と所在場所とをファイルインデックス記憶部１５に追加し、「ファイルの削除」があれば、そのファイル識別情報と所在場所とをファイルインデックス記憶部１５から削除し、「ファイルの名前変更」があれば、そのファイル識別情報を変更し、「移動」があればその所在場所を変更する。これによって、ファイルインデックス記憶部１５に記憶する、ファイル識別情報と所在場所の情報を最新の状態に保持することが出来る。

【0091】

そして所定のタイミングで、アクセス判定部７は、操作ログ情報記憶部６に記憶した操作ログ情報（または操作ログ情報受付部５で受け付けた操作ログ情報）について、操作内容として、ファイルへの所定のアクセス処理をした操作ログ情報が含まれているかを判定する（Ｓ１２０）。すなわち操作ログ情報の操作内容として、「ファイルの起動」、「ファイルを編集」、「コピー」、「移動」、「閲覧」などを含む操作ログ情報を判定する。

【0092】

このようにしてアクセス判定部７は、アクセス処理を操作内容として含む操作ログ情報のファイル識別情報とファイルの所在場所とを抽出する。なおこの際にアクセス判定部７は、アクセス処理を操作内容として含む操作ログ情報のファイル識別情報だけを操作ログ情報記憶部６から抽出し、ファイルの所在場所は、ファイルインデックス記憶部１５を参照することにより抽出しても良い。

【0093】

そしてアクセス判定部７は、抽出したファイル識別情報がすでに監視対象ファイル記憶部１０に登録されているかを確認し（Ｓ１３０）、監視対象ファイルとして登録されていなければ、抽出したファイル所在場所のファイルサーバ３、所定のサーバ、クライアント端末４に対して、当該ファイル識別情報を渡すことで、当該ファイルが個人情報や機密情報を含むファイルであるかの検索要求を検索要求部８が行う。この検索要求を受けた、当該ファイルを記憶するファイルサーバ３、所定のサーバ、クライアント端末４は、検索処理部で、当該ファイル識別情報を有するファイルに、個人情報や機密情報を含んでいるかを検索し（Ｓ１４０）、その結果を管理サーバ２に返す（Ｓ１５０）。

【0094】

一方、Ｓ１３０において、抽出したファイル識別情報がすでに監視対象ファイル記憶部１０に登録されている場合には、抽出したファイル識別情報の類似ファイル、関連ファイルの検索処理を実行する。すなわちＳ１７０以降の処理を実行することとなる。

【0095】

Ｓ１５０における検索結果として、前記抽出したファイル識別情報のファイルが、個人情報や機密情報を含んでいるファイルであることを受け取ると、監視対象ファイル登録処理部９は、新たに監視対象ファイルとして、そのファイル識別情報と所在場所とを監視対

象ファイル記憶部１０に記憶する（Ｓ１６０）。なおこの登録の前に、再度、監視対象ファイル記憶部１０に当該ファイル識別情報が登録されていないかの重複チェックを行っても良い。またＳ１３０における登録チェックや重複チェックの際には、同一のファイル識別情報を異なるクライアント端末４やファイルサーバ３などで使用していることが考えられるので、ファイル識別情報のみならず、ファイルの所在場所も検索キーとして使用して検索することが好ましい。つまりファイル識別情報と所在場所とが一致した場合には、すでに登録されているファイルと判定し、そうでなければ新たに監視対象ファイルとして追加すればよい。

【0096】

また検索結果として、個人情報や機密情報を含んでいるファイルであることを受け取ると、類似ファイル検索部１１が類似ファイル検索をファイルインデックス記憶部１５で実行し、また関連ファイル検索部１２が関連ファイル検索を操作ログ情報記憶部６で実行する（Ｓ１７０）。そして類似ファイル、関連ファイルが検索できたら、類似ファイル検索部１１、関連ファイル検索部１２は、その類似ファイル、関連ファイルの各ファイル識別情報がすでに監視対象ファイル記憶部１０に登録されているかを確認し（Ｓ１８０）、それらが監視対象ファイルとして登録されていなければ、検索要求部８が、検索した類似ファイル、関連ファイルの所在場所であるファイルサーバ３、クライアント端末４、所定のサーバに対して、類似ファイル、関連ファイルのファイル識別情報を渡すことで、当該ファイルが個人情報や機密情報を含むファイルであるかの検索要求を行う。この検索要求を受けた、当該ファイルを記憶するファイルサーバ３、所定のサーバ、クライアント端末４は、検索処理部で、当該ファイル識別情報を有するファイルに、個人情報や機密情報を含んでいるかを検索し（Ｓ１９０）、その結果を管理サーバ２に返す（Ｓ２００）。

【0097】

一方、Ｓ１８０において、類似ファイル、関連ファイルとして検索した各ファイル識別情報がすでに監視対象ファイル記憶部１０に登録されている場合には、そのままＳ２２０以降の処理を実行する。

【0098】

このようにして類似ファイル、関連ファイルについての検索結果を監視対象ファイル登録処理部９で受け取ると、新たに監視対象ファイルとして、そのファイル識別情報と所在場所とを監視対象ファイル記憶部１０に記憶する（Ｓ２１０）。なおこの登録の前に、再度、監視対象ファイル記憶部１０に当該ファイル識別情報が登録されていないかの重複チェックを行っても良い。

【0099】

なおＳ１７０からＳ２１０までの処理を、更に類似ファイル、関連ファイルについての検索結果に対して行っても良い。また類似ファイル、関連ファイルの検索処理は、どちらを先に行っても良いし、並列して行っても良い。

【0100】

このようにして監視対象ファイル記憶部１０に、監視対象のファイルとして記憶されたファイルについて、監視処理部１３は、操作ログ情報を用いて監視を実行する（Ｓ２２０）。

【0101】

また監視処理部１３における監視処理は、常に行われていることが好ましい。

【産業上の利用可能性】

【0102】

本発明のファイル管理システム１を用いることによって、コンピュータシステムに出来るだけ負荷をかけないで、必要な個人情報や機密情報を含むファイルの所在場所を管理することが出来る。

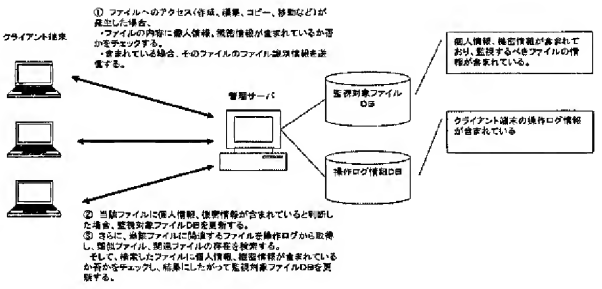
【図面の簡単な説明】

【0103】

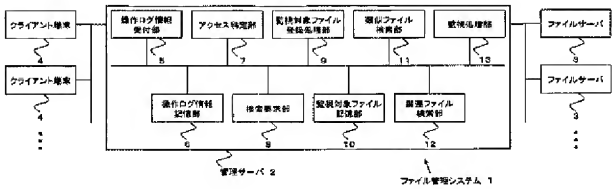
【図1】本発明の全体を模式的に示す図である。

【図2】本発明のシステム構成の一例を模式的に示す図である。
【図3】本発明のハードウェア構成の一例を模式的に示す図である。
【図4】本発明の処理プロセスの一例を示すフローチャートである。
【図5】機密情報のキーワードを記憶する保存部を模式的に示す図である。
【図6】操作ログ情報の一例を模式的に示す図である。
【図7】操作ログ情報記憶部の一例を模式的に示す図である。
【図8】操作ログ情報を用いてアクセス判定の処理を模式的に示す図である。
【図9】監視対象ファイル記憶部の一例を模式的に示す図である。
【図10】操作ログ情報を用いて類似ファイルの検索処理を模式的に示す図である。
【図11】操作ログ情報を用いて関連ファイルの検索処理を模式的に示す図である。
【図12】本発明のシステム構成の他の一例を模式的に示す図である。
【図13】ファイルインデックス記憶部の一例を模式的に示す図である。
【符号の説明】
【0104】
１：ファイル管理システム
２：管理サーバ
３：ファイルサーバ
４：クライアント端末
５：操作ログ情報受付部
６：操作ログ情報記憶部
７：アクセス判定部
８：検索要求部
９：監視対象ファイル登録処理部
１０：監視対象ファイル記憶部
１１：類似ファイル検索部
１２：関連ファイル検索部
１３：監視処理部
１４：ファイルインデックス処理部
１５：ファイルインデックス記憶部

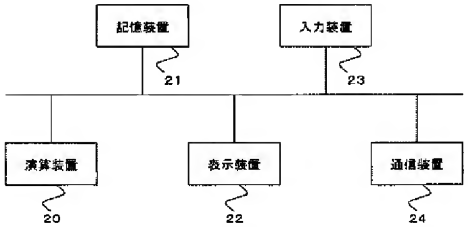
【図1】



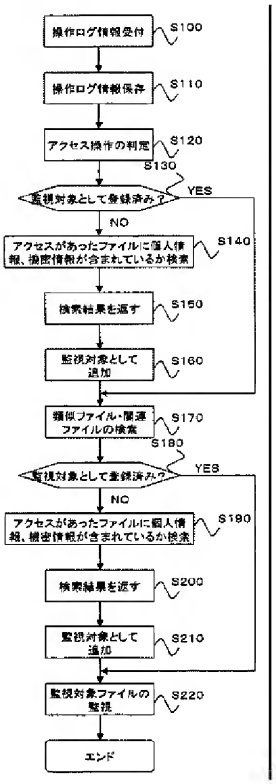
【図2】



【図3】



【図4】



【図5】

キーワード
○○○○（社員名）
××××（新商品名）
AAAA（開発中の新機能の名前）
CCCC（業務提携先の企業名）
・
・
・

【図6】

クライアント端末識別情報	日時	ログイン名	操作内容	ファイル識別情報	保存場所
ABC12345678	2007/1/30/13:11:15	XXXXX	ファイル読取	顧客情報一覧表	￥￥Tokyo－fs￥営業書類￥顧客

ファイルサーバ名　　ディレクトリ名

【図7】

クライアント端末識別情報	日時	ログイン名	操作内容	ファイル識別情報	保存場所
ABC12345678	2007/1/30/13:11:15	XXXXX	アクティブ	スタートメニュー	―
ABC12345678	2007/1/30/13:11:18	XXXXX	ファイル起動	顧客情報一覧表	￥￥Tokyo－fs￥営業書類￥顧客
ABC12345678	2007/1/30/13:11:19	XXXXX	アクティブ	予定表	C:¥Documents and Settings¥デスクトップ
ABC12345678	2007/1/30/13:11:20	XXXXX	ドライブ追加	リムーバブル	―
ABC12345678	2007/1/30/13:11:22	XXXXX	アクティブ	Microsoft Office Word	C:¥Documents and Settings¥デスクトップ
ABC12345678	2007/1/30/13:11:23	XXXXX	ファイル起動	一般公開プレゼン資料	￥￥Tokyo－fs￥公開用￥資料
ABC12345678	2007/1/30/13:11:24	XXXXX	アクティブ	予定表	C:¥Documents and Settings¥デスクトップ

【図8】

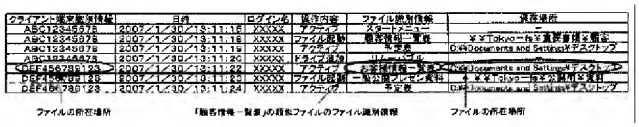
クライアント端末識別情報	日時	ログイン名	操作内容	ファイル識別情報	保存場所
ABC12345678	2007/1/30/13:11:15	XXXXX	アクティブ	スタートメニュー	―
ABC12345678	2007/1/30/13:11:18	XXXXX	ファイル起動	顧客情報一覧表	￥￥Tokyo－fs￥営業書類￥顧客
ABC12345678	2007/1/30/13:11:19	XXXXX	アクティブ	予定表	C:¥Documents and Settings¥デスクトップ
ABC12345678	2007/1/30/13:11:20	XXXXX	ドライブ追加	リムーバブル	―
ABC12345678	2007/1/30/13:11:22	XXXXX	アクティブ	Microsoft Office Word	C:¥Documents and Settings¥デスクトップ
ABC12345678	2007/1/30/13:11:23	XXXXX	ファイル起動	一般公開プレゼン資料	￥￥Tokyo－fs￥公開用￥資料
ABC12345678	2007/1/30/13:11:24	XXXXX	アクティブ	予定表	C:¥Documents and Settings¥デスクトップ

ファイルへのアクセス結果　　アクセスしたファイルのファイル識別情報

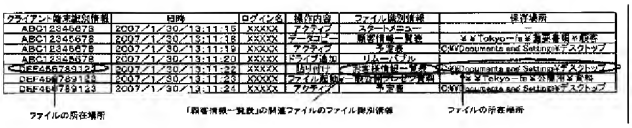
【図9】

ファイル識別情報	保存場所
営業記録	クライアント端末（AAA）
顧客情報一覧表	ファイルサーバ（Tokyo－fs）
社員名簿	ファイルサーバ（Osaka－fs）
・	・
・	・
・	・

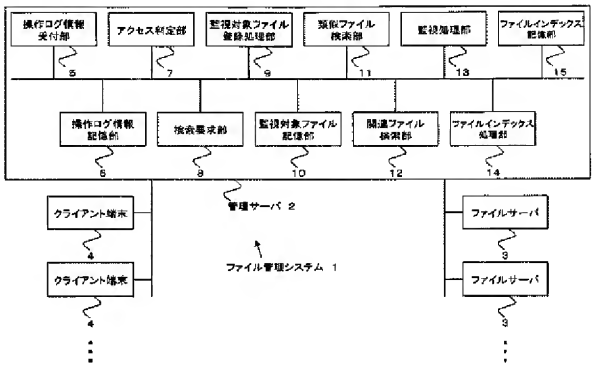
【図10】



【図11】



【図12】



【図13】

ファイル識別情報	保存場所
新商品説明会用資料	クライアント端末(AAA)
機能情報一覧表	クライアント端末(AAA)
営業記録	クライアント端末(AAA)
一般公開プレゼン用資料	ファイルサーバ(Tokyo－fs)
ミーティング議事録	クライアント端末(BBB)
顧客情報一覧表	ファイルサーバ(Tokyo－fs)
ソフトウェア開発要求仕様書	ファイルサーバ(Tokyo－fs)
社員名簿	ファイルサーバ(Osaka－fs)
開発委託契約書	ファイルサーバ(Nagoya－fs)
・	・
・	・
・	・